ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Microsoft OneDrive accounts connected to the following email addresses that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at 1 Microsoft Way, Redmond, WA 98052:

a. jsnmcsweeney@outlook.com,
b. jsnmcsweeney1@outlook.com,
c. jsndlvmcs@outlook.com, and
d. fortextnowjsnmcs@outlook.com.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation ("Microsoft")

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that has been deleted but is still available to Microsoft, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A (the "TARGET ACCOUNTS") for the time period from inception to present:

a. For the time period inception to present, the contents of all communications and related transactional records for all Microsoft OneDrive services associated with the TARGET ACCOUNTS, including but not limited to incoming, outgoing, and draft emails, messages, calls, chats, posts, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

b. For the time period inception to present, the contents of all other data and related transactional records for all Microsoft OneDrive

services used by the TARGET ACCOUNTS, including any information ever generated, modified, or stored by user(s) or Microsoft in connection with the TARGET ACCOUNTS (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

c. For the time period inception to present, all records of online search and browsing history associated with the TARGET ACCOUNTS or their users (including information collected through tracking cookies);

d. For the time period inception to present, all records and other information concerning any document, website, or other computer file created, stored, revised, or accessed by the TARGET ACCOUNTS or by their users, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

e. For the time period inception to present, all records regarding identification of the TARGET ACCOUNTS, including the names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration

(including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

f. For the time period inception to present, all device or user identifiers which have ever been linked to the TARGET ACCOUNTS, including but not limited to all cookies and similar technologies, Android ID, Advertising ID, unique application number, hardware model, operating system version, device serial number, Global Unique Identifier ("GUID"), mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI");

g. All records or other information regarding the identification of the TARGET ACCOUNTS, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

h. For the time period inception to present, all records of communications between Microsoft and any person regarding the TARGET ACCOUNTS, including contacts with support services and records of actions taken;

i. For the time period inception to present, information about any complaint, alert or other terms of service violation related to the

TARGET ACCOUNTS or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the TARGET ACCOUNTS or associated user(s) (but not including confidential communications with legal counsel); and

j. For the time period inception to present, for all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

Microsoft is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B) (the "Subject Offenses") committed by Jason Doliver MCSWEENEY since the inception of the TARGET ACCOUNTS, including information pertaining to the following matters:

a. Any child pornography and/or child erotica that was sent, received, or possessed by the TARGET ACCOUNTS and information pertaining to the context of the transmission of child pornography and/or child erotica to or from the TARGET ACCOUNTS;

b. Any communications related to or regarding the production, receipt, distribution, or possession of child pornography and/or child erotica;

c. The identity of the person(s) who communicated with the TARGET ACCOUNTS about matters relating to the production, transfer, receipt,

distribution, and possession of child pornography, including records that help reveal the whereabouts of such person(s);

d. The identity of the person(s) who created or used the TARGET ACCOUNTS, including records that help reveal the whereabouts of such person(s);

e. How and when the TARGET ACCOUNTS was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and the owner(s) of the TARGET ACCOUNTS; and

f. The state of mind of the owner(s) of the TARGET ACCOUNTS as it relates to the crimes under investigation.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.